Содержание:

Введение

Современная сеть передачи данных – это множество удаленных высокопроизводительных устройств, взаимодействующих друг с другом на значительном расстоянии. Одними из наиболее крупномасштабных сетей передачи данных являются компьютерные сети, такие как сеть Интернет. В ней одновременно работают миллионы источников и потребителей информации по всему миру. Широкое развитие данной сети позволяет использовать ее не только частным лицам, но и крупным компаниям для объединения своих разрозненных устройств по всему миру в единую сеть.

Вместе с этим, общий доступ к единым физическим ресурсам открывает доступ мошенникам, вирусам и конкурентам возможность причинить вред конечным пользователям: похитить, исказить, подбросить или уничтожить хранимую информацию, нарушить целостность программного обеспечения и даже вывести аппаратную часть конечной станции.

Для предотвращения данных нежелательных воздействий необходимо предотвратить несанкционированный доступ, для чего часто применяется Firewall. Само название Firewall (wall – от англ. стена) кроет в себе его назначение, т.е. он служит стеной между защищаемой локальной сетью и Интернетом либо любой другой внешней сетью и предотвращать любые угрозы.

Кроме вышеуказанной межсетевой экран также может выполнять и другие функции, связанные с фильтрацией трафика от/к какому-либо ресурсу сети Интернет.

Тема работы: Брандмауэр. Назначение, специфика настройки, принцип использования

Цель данной работы –.Изучить назначение, специфику настройки, принцип использования брандмауэров.

Объектом исследования. Брандмауэр.

Предметом исследования является Назначение, специфику настройки, принцип использования брандмауэров.

Задачи исследования: изучить

Определение межсетевого экрана или брандмауэра

История создания брандмауэров

Фильтрация трафика

Классификация межсетевых экранов или брандмауэров

Формы межсетевых экранов

Реализация брандмауэров

Ограничения межсетевого экрана

Классы защищенности брандмауэров

Стандартизация брандмауэров

Настройка брандмауэров

Глава 1. Описание межсетевых экранов

1.1 Определение межсетевого экрана

Межсетевой экран или брандмауэр — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.

Межсетевые экраны используются в качестве первой линии защиты сетей уже более 25 лет. Они ставят барьер между защищенными, контролируемыми внутренними сетями, которым можно доверять, и ненадежными внешними сетями, такими как Интернет.

Рис 1.1 Межсетевой экран

Сетевой экран используется для защиты отдельных сегментов сети или хостов от возможного несанкционированного проникновения через уязвимости программного обеспечения, установленного на ПК, или протоколов сети. Работа межсетевого крана заключается в сравнении характеристик проходящего сквозь него трафика с шаблонами уже известного вредоносного кода [8].

Наиболее часто брандмауэр инсталлируется на границе периметра локальной сети, где он выполняет защиту внутренних узлов. Тем не менее, атаки могут инициироваться изнутри, поэтому при атаке на сервер той же сети, межсетевой экран не воспримет это как угрозу. Это стало причиной, по которой брандмауэры стали устанавливать не только на границе сети, но и между её сегментами, что значительно повышает степень безопасности сети.

1.2 История создания

Свою историю брандмауэры начинают с конца восьмидесятых прошлого века, когда Интернет ещё не стал повседневной вещью для большинства людей. Их функцию выполняли маршрутизаторы, осуществлявшие анализ трафика на основе данных из протокола сетевого уровня. Затем, с развитием сетевых технологий, эти устройства смогли использовать данные уже транспортного уровня. По сути, маршрутизатор являет собой самую первую в мире реализацию программно-аппаратного брандмауэра.

Программные сетевые экраны возникли много позже. Так, Netfilter/iptables, межсетевой экран для Linux, был создан только в 1998 году. Связано это с тем, что ранее функцию фаейрвола выполняли, и весьма успешно, антивирусные программы, но с конца 90-х вирусы усложнились, и появление межсетевого экрана стало необходимым [4].

1.3 Фильтрация трафика

Трафик фильтруется на основе заданных правил – ruleset. По сути, межсетевой экран представляет собой последовательность анализирующих и обрабатываемых трафик фильтров согласно данному пакету конфигураций. У каждого фильтра своё назначение; причём, последовательность правил может значительно влиять на производительность экрана. К примеру, большинство файрволов при анализе трафика последовательно сравнивают его с известными шаблонами из списка – очевидно, что наиболее популярные виды должны располагаться как можно выше.

Принципов, по которому осуществляется обработка входящего трафика, бывает два. Согласно первому разрешаются любые пакеты данных, кроме запрещённых, поэтому если он не попал ни под какое ограничение из списка конфигураций, он передается далее. Согласно второму принципу, разрешаются только те данные, которые не запрещены – такой метод обеспечивает самую высокую степень защищенности, однако существенно нагружает администратора.

Брандмауэр выполняет две функции: deny, запрет данных – и allow – разрешение на дальнейшую передачу пакет. Некоторые брандмауэры способны выполнять также операцию reject – запретить трафик, но сообщить отправителю о недоступности сервиса, чего не происходит при выполнении операции deny, обеспечивающей таким образом большую защиту хоста [3].

1.4 Классификация межсетевых экранов или брандмауэров

Чаще всего межсетевые экраны классифицируют по поддерживаемому уровню сетевой модели OSI. Различают:

Управляемые коммутаторы;

Пакетные фильтры;

Шлюзы сеансового уровня;

Посредники прикладного уровня;

Инспекторы состояния.

Управляемые коммутаторы

Нередко причисляются к классу межсетевых экранов, но осуществляют свою функцию на канальном уровне, поэтому не способны обработать внешний трафик.

Некоторые производители (ZyXEL, Cisco) добавили в свой продукт возможность обработки данных на основе MAC-адресов, которые содержатся в заголовках фреймов. Тем не менее, даже этот метод не всегда приносит ожидаемый результат, так как мак-адрес можно легко изменить с помощью специальных программ. В связи с этим в наши дни коммутаторы чаще всего ориентируются на другие показатели, а именно на VLAN ID.

Виртуальные локальные сети позволяют организовывать группы хостов, в которые данные стопроцентно изолированы от внешних серверов сети.

В рамках корпоративных сетей управляемые коммутаторы могут стать весьма эффективным и сравнительно недорогим решением. Главным их минусом является неспособность обрабатывать протоколы более высоких уровней [11].

Пакетные фильтры

Пакетные фильтры используются на сетевом уровне, осуществляя контроль трафика на основе данных из заголовка пакетов. Нередко способны обрабатывать также заголовки протоколов и более высокого уровня – транспортного (UDP, TCP), Пакетные фильтры стали самыми первыми межсетевыми экранами, остаются самыми популярными и на сегодняшний день. При получении входящего трафика анализируются такие данные, как: IP получателя и отправителя, тип протокола, порты получателя и источника, служебные заголовки сетевого и транспортного протоколов.

Уязвимость пакетных фильтров заключается в том, что они могут пропустить вредоносный код, если он разделен на сегменты: пакеты выдают себя за часть другого, разрешённого контента. Решение этой проблемы заключается в блокировании фрагментированных данных, некоторые экраны способны также дефрагментировать их на собственном шлюзе – до отправки в основной узел сети. Тем не менее, даже в этом случае межсетевой экран может стать жертвой DDos-атаки.

Пакетные фильтры реализуются в качестве компонентов ОС, пограничных маршрутизаторов или персональных сетевых экранов [1].

Пакетные фильтры отличаются высокой скоростью анализа пакетов, отлично выполняют свои функции на границах с сетями низкой степени доверия. Тем не менее, они неспособны анализировать высокие уровни протоколов и легко могут жертвами атак, при которых подделывается сетевой адрес.

Шлюзы сеансового уровня

Использование сетевого экрана позволяет исключить прямое взаимодействие внешних серверов с узлом – в данном случае он играет роль посредника, называемого прокси. Он проверяет каждый входящий пакет, не пропуская те, что не принадлежат установленному ранее соединению. Те пакеты, которые выдают себя за пакеты уже завершённого соединения, отбрасываются.

Шлюз сеансового уровня – единственное связующее звено между внешней и внутренней сетями. Таким образом, определить топологию сети, которую защищает шлюз сеансового уровня, становится затруднительно, что значительно повышает её защищённость от DoS-атак.

Тем не менее, даже у этого решения есть значительный минус: ввиду отсутствия возможности проверки содержания поля данных хакер относительно легко может передать в защищаемую сеть трояны [10].

Посредники прикладного уровня

Как и шлюзы сеансового уровня, фаейрволы прикладного уровня осуществляют посредничество между двумя узлами, но отличаются существенным преимуществом – способностью анализировать контекст передаваемых данных. Сетевой экран подобного типа может определять и блокировать нежелательные и несуществующие последовательности команд (подобное часто означает ДОС-атаку), а также запрещать некоторые из них вообще.

Посредники прикладного уровня определяют и тип передаваемой информации – ярким примером являются почтовые службы, запрещающие передачу исполняемых файлов. Кроме этого они могут осуществлять аутентификацию пользователя, наличие у SSL-сертификатов подписи от конкретного центра.

Главным минусом такого типа сетевого экрана является долгий анализ пакетов, требующий серьёзных временных затрат. Помимо этого, у посредников прикладного уровня нет автоподключения поддержки новых протоколов и сетевых приложений.

Инспекторы состояния

Создатели инспекторов состояния поставили перед собой цель собрать воедино преимущества каждого их выше перечисленных типов сетевых экранов, получив таким образом брандмауэр, способный обрабатывать трафик как на сетевом, так и на прикладном уровнях.

Инспекторы состояния осуществляют контроль:

всех сессий – основываясь на таблице состояний,

всех передаваемых пакетов данных – на основе заданной таблицы правил,

всех приложений, на основе разработанных посредников.

Фильтрация трафика инспектора состояния происходит тем же образом, что и при использовании шлюзов сеансового уровня, благодаря чему его производительность гораздо выше, чем у посредников прикладного уровня. Инспекторы состояния отличаются удобным и понятным интерфейсом, лёгкой настройкой, обладают широкими возможностями расширения.

Также межсетевые экраны могут классифицироваться следующим образом:

Прокси-сервер

Это один из первых типов МСЭ. Прокси-сервер служит шлюзом между сетями для конкретного приложения. Прокси-серверы могут выполнять дополнительные функции, например кэширование и защиту контента, препятствуя прямым подключениям из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

Межсетевой экран с контролем состояния сеансов

Сегодня МСЭ с контролем состояния сеансов считается «традиционным». Он пропускает или блокирует трафик с учетом состояния, порта и протокола. Он осуществляет мониторинг всей активности с момента открытия соединения и до его закрытия. Решения о фильтрации принимаются на основании как правил, определяемых администратором, так и контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению [5].

Межсетевой экран UTM

Типичное устройство UTM, как правило, сочетает такие функции, как контроль состояния сеансов, предотвращение вторжений и антивирусное сканирование. Также оно может включать в себя дополнительные службы, а зачастую — и управление облаком. Основные достоинства UTM — простота и удобство.

Межсетевой экран нового поколения (NGFW)

Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем состояния сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений.

Согласно определению компании Gartner, Inc., межсетевой экран нового поколения должен иметь:

стандартные функции МСЭ, такие как контроль состояния сеансов;

встроенную систему предотвращения вторжений;

функции учета и контроля особенностей приложений, позволяющие распознавать и блокировать приложения, представляющие опасность;

схему обновления, позволяющую учитывать будущие каналы информации;

технологии защиты от постоянно меняющихся и усложняющихся угроз безопасности.

И хотя эти возможности постепенно становятся стандартными для большинства компаний, межсетевые экраны нового поколения способны на большее.

NGFW с активной защитой от угроз

Эти межсетевые экраны сочетают в себе функции традиционного NGFW с возможностями обнаружения и нейтрализации сложных угроз. Межсетевые экраны нового поколения с активной защитой от угроз позволяют:

определять благодаря полному учету контекста, какие ресурсы наиболее подвержены риску;

быстро реагировать на атаки благодаря интеллектуальной автоматизации безопасности, которая устанавливает политики и регулирует защиту в динамическом режиме;

с большей надежностью выявлять отвлекающую или подозрительную деятельность, применяя корреляцию событий в сети и на оконечных устройствах;

значительно сократить время с момента распознавания до восстановления благодаря использованию ретроспективных средств обеспечения безопасности, которые осуществляют непрерывный мониторинг на предмет подозрительной деятельности и поведения даже после первоначальной проверки;

упростить администрирование и снизить уровень сложности с помощью унифицированных политик, обеспечивающих защиту на протяжении всего жизненного цикла атаки.

1.5 Формы межсетевых экранов

Решения для межсетевых экранов поставляются в различных формах:

Аппаратные межсетевые экраны. Аппаратный межсетевой экран – это выделенное устройство, называемое устройством защиты.

Серверные межсетевые экраны. Серверный межсетевой экран представляет собой приложение межсетевого экрана, выполняемое в сетевой операционной системе (NOS), например, **UNIX**, Windows или Novell.

Интегрированные межсетевые экраны. Интегрированный межсетевой экран дополняет возможности существующего устройства (например, маршрутизатора) функциями межсетевого экрана.

Персональные межсетевые экраны. Персональные межсетевые экраны размещаются на узлах и не рассчитаны на защиту локальной сети в целом. Они могут быть реализованы в ОС по умолчанию или установлены сторонним поставщиком.

1.6 Реализация межсетевых экранов

Межсетевые экраны (Firewall) могут быть либо программно-аппаратными, ибо программными. Первые могут быть выполнены как в виде отдельного модуля в маршрутизаторе или коммутаторе, так и специального устройства.

Чаще всего пользователи выбирают исключительно программные межсетевые экраны – по той причине, что для их использования достаточно лишь установки специального софта. Тем не менее, в организациях нередко найти свободный компьютер под заданную цель, бывает затруднительно – к тому же, отвечающий всем техническим требованиям, зачастую довольно высоким [7].

Именно поэтому крупные компании предпочитают установку специализированных программно-аппаратных комплексов, получивших название «security appliance». Работают они чаще всего на основе систем Linux или же FreeBSD, ограниченных функционалом для выполнения заданной функции.

Такое решение имеет следующие преимущества:

Лёгкое и просто управление: контроль работы программно-аппаратного комплекса осуществляется с любого стандартного протокола (Telnet, SNMP) – или защищённого (SSL, SSH).

Высокая производительность: работа операционной системы направлена на одну единственную функцию, из неё исключены любые посторонние сервисы.

Отказоустойчивость: программно-аппаратные комплексы эффективно выполняют свою задачу, вероятность сбоя практически исключена.

1.7 Ограничения межсетевого экрана

Сетевой экран не проводит фильтрацию тех данных, которые не может интерпретировать. Пользователь сам настраивает, что делать с нераспознанными данными – в файле конфигураций, согласно которым и осуществляется обработка такого трафика. К таким пакетам данным относятся трафик из протоколов SRTP, IPsec, SSH, TLS, которые используют криптографию для скрытия содержимого, протоколы, шифрующие данные прикладного уровня (S/MIME и OpenPGP). Также невозможна фильтрация туннелирования трафика, если механизм того туннелирования непонятен сетевому экрану. Значительная часть недостатков межсетевых экранов исправлена в UTM-системах - Unified Threat Management, иногда их так же называют NextGen Firewall.

1.8 Классы защищенности брандмауэров

Существуют три группы на которых делят АС по обработке конфиденциальной информации:

Многопользовательские АС, они обрабатывают данные различных уровней конфиденциальности

Многопользовательские АС, где пользователи имеют одинаковый доступ к обрабатываемой информации, которые находятся на носителях разного уровня доступа

Однопользовательские АС, пользователь имеет полный доступ ко всем обрабатываемой информации, которая находится на носителях разного уровня конфиденциальности

В первой группе держат 5 классов защищенности АС: 1А, 1Б, 1В, 1Г, 1Д, во второй и третьей группах — 2А, 2Б и 3А, 3Б. Класс А соответствует максимальной, класс Д — минимальной защищенности АС. Брандмауэры разрешают реализовывать безопасность объектов внутренней части, игнорируя несанкционированные запросы из внешней части сети — реализуют *экранирование*.

Проблемы безопасности МЭ

МЭ не может решать все проблемы и погрешности в корпоративной сети. Кроме описанных выше достоинств, есть ущемление в их эксплуатации и угрозы безопасности, от которых МЭ не могут защитить. Наиболее существенные описаны ниже:

отсутствие защиты от вирусов. Обычные МЭ не могут защитить от особей, которые загружают зараженные вирусами программы для ПК из интернета или при передаче таких программ в приложенных в письме, поскольку эти программы могут быть зашифрованы или сжаты большим числом способов;

возможное ограничение пропускной скорости. Обычные МЭ являются потенциально узким узлом в сети, так как все пакеты передаваемые из внешней сети во внутреннюю должны проходить через МЭ;

отсутствие эффективной защиты от опасного содержимого (управляющие элементы ActiveX, апплеты Java, сценарии JavaScript и т.п.).

Эффективным было бы не только запрещение, но и упреждение атак, т.е. предотвращение предпосылок совершения вторжений. Для организации

предотвращение атак необходимо реализовывать средства поиска уязвимостей и обнаружения атак, которые будут вовремя раскрывать и рекомендовать меры по изъятию «слабых мест» в системе защиты.

Общепринятые МЭ являются по существу средствами, только блокирующими атаки. Впринципи они защищают от атак, которые уже находятся в процессе осуществления [9].

МЭ к сожалению не может защитить от некомпетентности и погрешности пользователей и администраторов;

Для защиты информационных ресурсных фондов поделенных корпоративных систем нужно применить комплексный подход защиты информационной безопасности, которая разрешит эффективно применить достоинства МЭ и компенсировать недостатки с помощью других средств безопасности.

Руководство составлено специально для оборудования Check Point, однако оно также может быть использовано, как основа для самостоятельного аудита сети, построенной на оборудовании других вендоров (Cisco, Fortinet, Palo Alto и т.д.).

Глава 2 Стандартизация брандмауэров

Согласно Информационному сообщению «Об утверждении методических документов, содержащих профили защиты межсетевых экранов» от 12 сентября 2016 г. N 240/24/4278 разработаны Профили защиты типов: межсетевой экран уровня сети (тип «А») – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы. Межсетевые экраны типа «А» могут иметь только программно-техническое исполнение;

- межсетевой экран уровня логических границ сети (тип «Б») – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы. Межсетевые экраны типа «Б» могут иметь программное или программно-техническое исполнение;
- межсетевой экран уровня узла (тип «В») – межсетевой экран, применяемый на узле (хосте) информационной системы. Межсетевые экраны типа «В» могут иметь только программное исполнение и устанавливаются на мобильных или

стационарных технических средствах конкретного узла информационной системы;

- межсетевой экран уровня веб-сервера (тип «Г») – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;
- межсетевой экран уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы).

Для типов А, Б и В имеются требования к межсетевым экранам от первого до шестого класса защиты, для типов Г и Д — только от шестого до четвертого.

Межсетевые экраны, соответствующие 6 классу защиты, применяются в государственных информационных системах 3 и 4 классов защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровней защищенности персональных данных.

Межсетевые экраны, соответствующие 5 классу защиты, применяются в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных [10].

Межсетевые экраны, соответствующие 4 классу защиты, применяются в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня

защищенности персональных данных, в информационных системах общего пользования II класса.

Глава 3 Настройка брандмауэра

Вообще говоря, в случае с Check Point аудит «правильности» настроек можно выполнять в автоматическом режиме. Осуществляется это с помощью программного блейда Compliance, который активируется на менеджмент сервере:

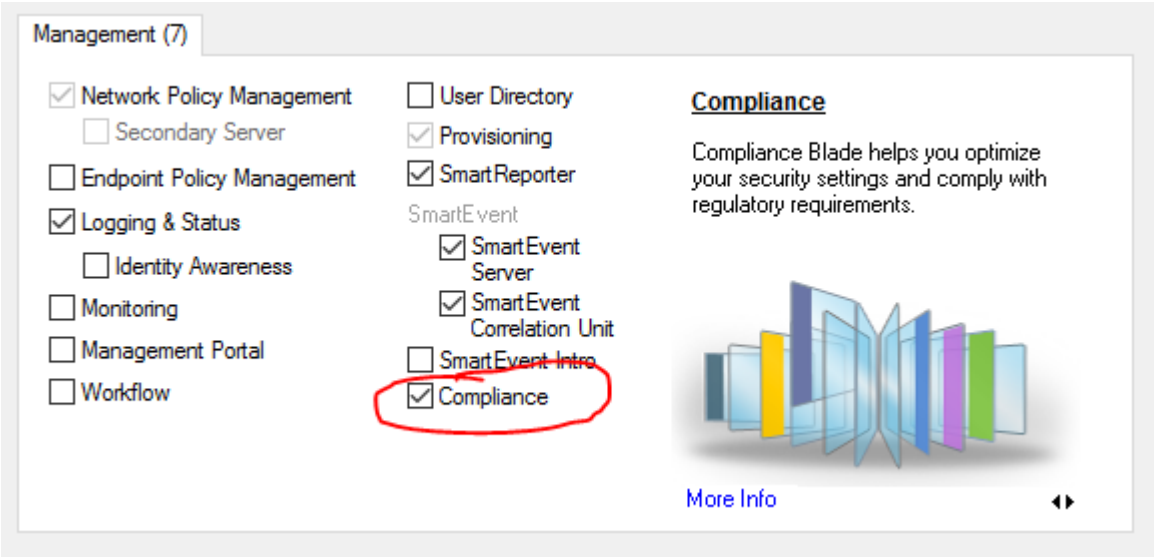


Рис.2.1 Настройка программного блейда Compliance

Данный блейд выполняет следующие функции:

Мониторинг программных блейдов в режиме 24/7

Постоянный контроль за тем, чтобы система управления, программные блейды и шлюзы безопасности были настроены оптимально.

Показывает неправильные настройки конфигурации и уязвимости в защите.

Предоставляет рекомендации по укреплению безопасности.

Уведомления в режиме реального времени

Показывает, как изменение конфигурации повлияет на безопасность.

Уведомляет об изменениях политик, негативно влияющих на безопасность.

Обучает пользователей, какими будут последствия желаемых изменений.

Готовые отчеты

Переводит тысячи требований регуляторов на язык практических рекомендаций.

Постоянная оценка совместимости с требованиями регуляторов (PCI DSS, ISO, NIST, DSD и так далее).

Все отчеты отображаются в графическом виде:

Оценка настроек:

Рис. 2.2 Оценка настроек

Оценка соответствия требованиям регуляторов:

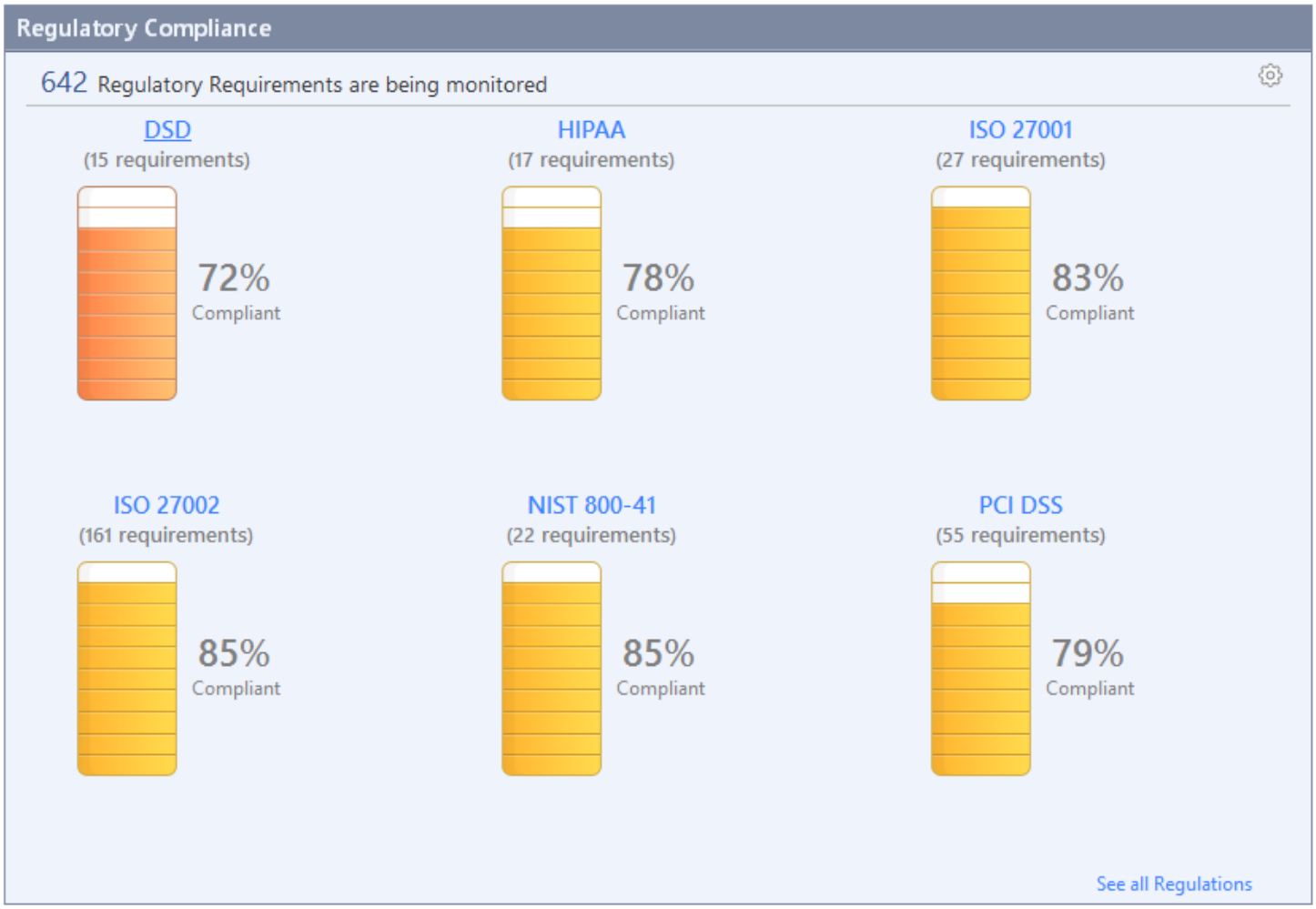


Рис.2.3 Оценка соответствия требованиям регуляторов

Оценка производительности отдельных шлюзов и блейдов:

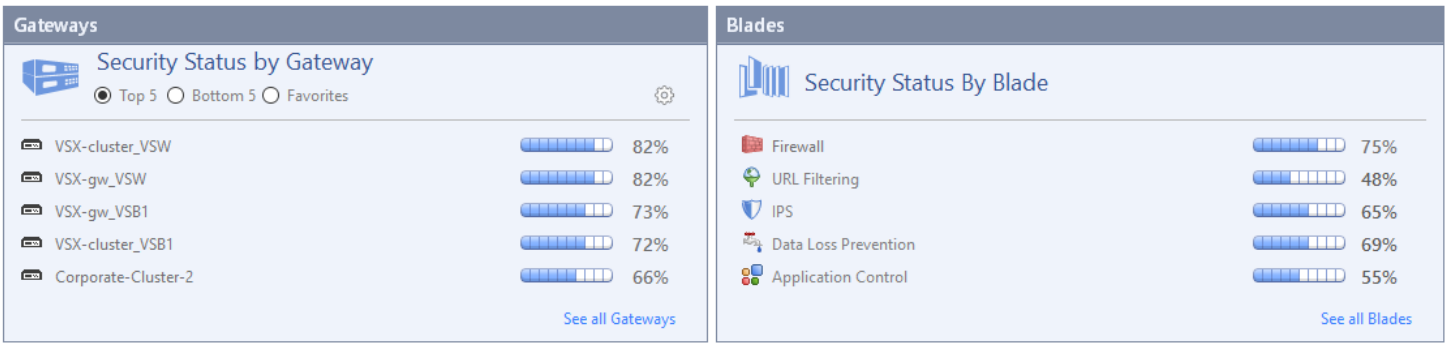


Рис. 2.4 Оценка производительности отдельных шлюзов и блейдов

Блейд Compliance поставляется бесплатно с подпиской на 1 год при покупке сервера управления (будь то физический appliance Smart-1 или виртуальная машина). Этого времени вполне достаточно для комплексной настройки средств защиты с последующей оценкой конфигураций. Таким образом, в первый год вы

получаете бесплатный аудит сетевой безопасности (настроек Check Point).

Если вы еще ни разу не активировали данный блейд, то это весьма просто сделать в свойствах сервера управления (Management Server), как это было показано на картинке выше. После этого проинсталлировать политики и подождать некоторое время (в зависимости от размеров сети и количества шлюзов). С результатом оценки конфигураций можно ознакомиться на соответствующей вкладке Compliance в консоли SmartDashboard:

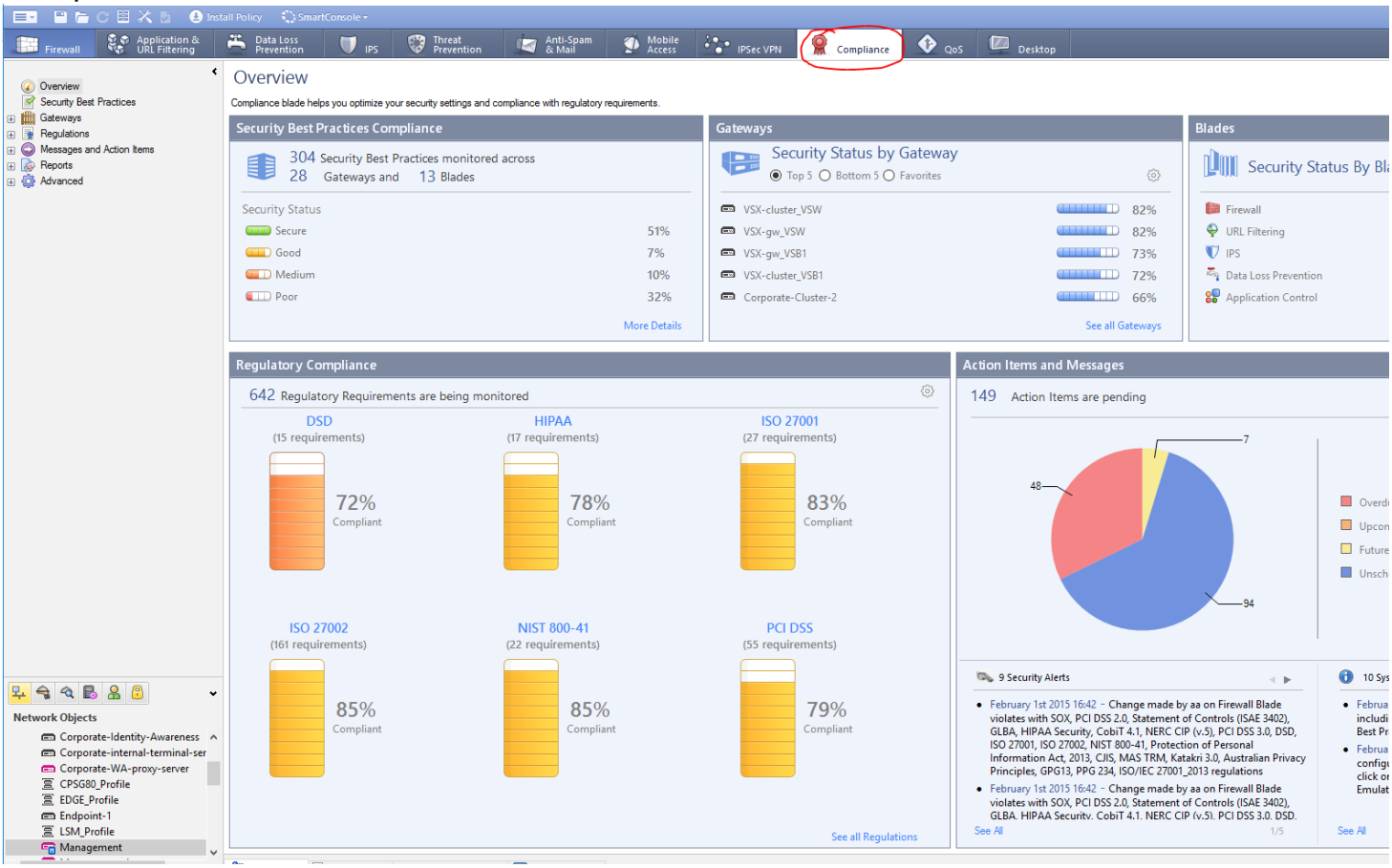


Рис. 2.5 Оценка конфигурации

Проверка безопасности текущих настроек в соответствии с рекомендациями Check Point.

Firewall Best Practices

1. Присутствует правило Management (название может отличаться):

Name	Source	Destination	VPN	Service	Action	Track
Management	Management Admin	Corporate-gw	Any Traffic	TCP ssh TCP https	accept	Lo

Рис. 2.6 Правило Management

Данное правило используется для доступа с сервера управления (Management Server) и компьютера администратора к шлюзу безопасности (Security Gateway). Остальным доступ должен быть запрещен.

2. Присутствует правило Stealth (название может отличаться):

Рис. 2.7 Правило Stealth

Данное правило используется для блокирования любой попытки доступа к самому шлюзу, что делает его “невидимым” и исключает возможность несанкционированного доступа. Убедитесь, что это правило расположено ниже чем Management.

3. Присутствует правило Clean up rule (название может отличаться):

Рис. 2.8 Правило Clean up rule

По умолчанию Check Point блокирует все соединения, которые явно не разрешены. Данное правило используется исключительно для логирования всех пакетов, которые и без этого были бы заблокированы. Правило должно быть самым последним в списке.

4. Присутствует правило Do Not Log (название может отличаться) для которого отключено логирование:

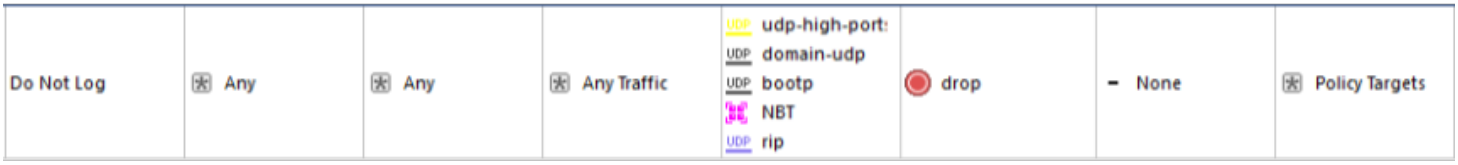


Рис. 2.9 Правило Do Not Log

Данное правило используется для фильтрования “паразитного” широковещательного трафика. К такому трафику относятся: udp-high-ports (UDP ports > 1024-65535), domain-udp, bootp, NBT (NetBios), rip (список может отличаться, в зависимости от вашей сети). Логирование отключается намеренно, дабы не

перегружать логи межсетевого экрана бесполезной информацией. Правило должно находиться как можно выше в списке (лучше первым).

5. В списках доступа в колонке источник (source) отсутствует значение Any, т.е. любой трафик. Всегда указывайте конкретный источник в правилах, будь то сеть или хост. За исключением правил Stealth, Clean up rule, Do Not Log.

6. Отсутствуют правила разрешающие весь трафик (any any accept).

7. Запрещен входящий Internet трафик для сегментов Бухгалтерии (Finance) и Отдела кадров (HR).

8. Запрещен FTP трафик из сети Internet в DMZ.

9. Отсутствуют неиспользуемые правила. В консоли SmartDashboard можно просматривать счетчик совпадений по каждому списку доступа:

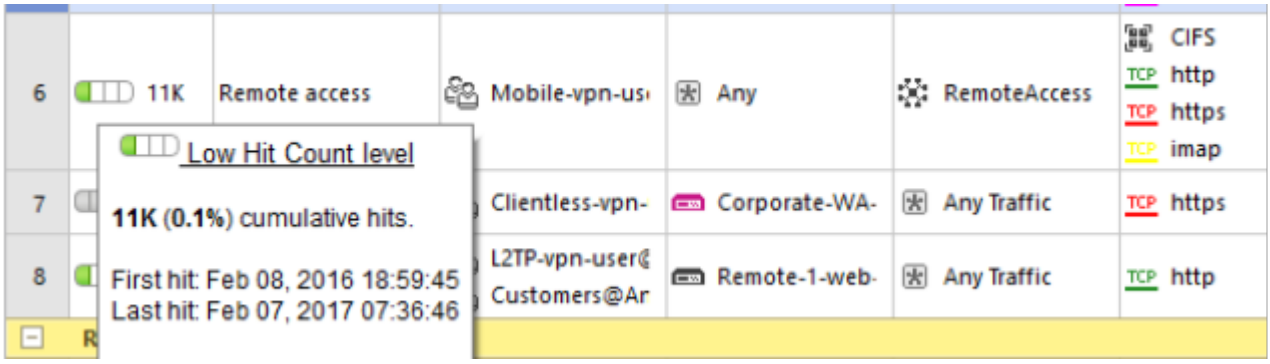


Рис. 2.10 Счетчик совпадений

Если счетчик показывает нулевое значение или последнее совпадение (Last hit) было более чем 6 месяцев назад, то рекомендуется удалить данное правило, дабы не перегружать общий список.

10. Для всех правил в поле Track выставлена опция Log. Кроме правила Do Not Log. Так вы сможете логировать все важные события исключая широковещательный трафик.

11. Для всех правил указано “адекватное” имя и присутствует комментарий, поясняющий назначение этого правила.

12. На всех шлюзах включено логирование.

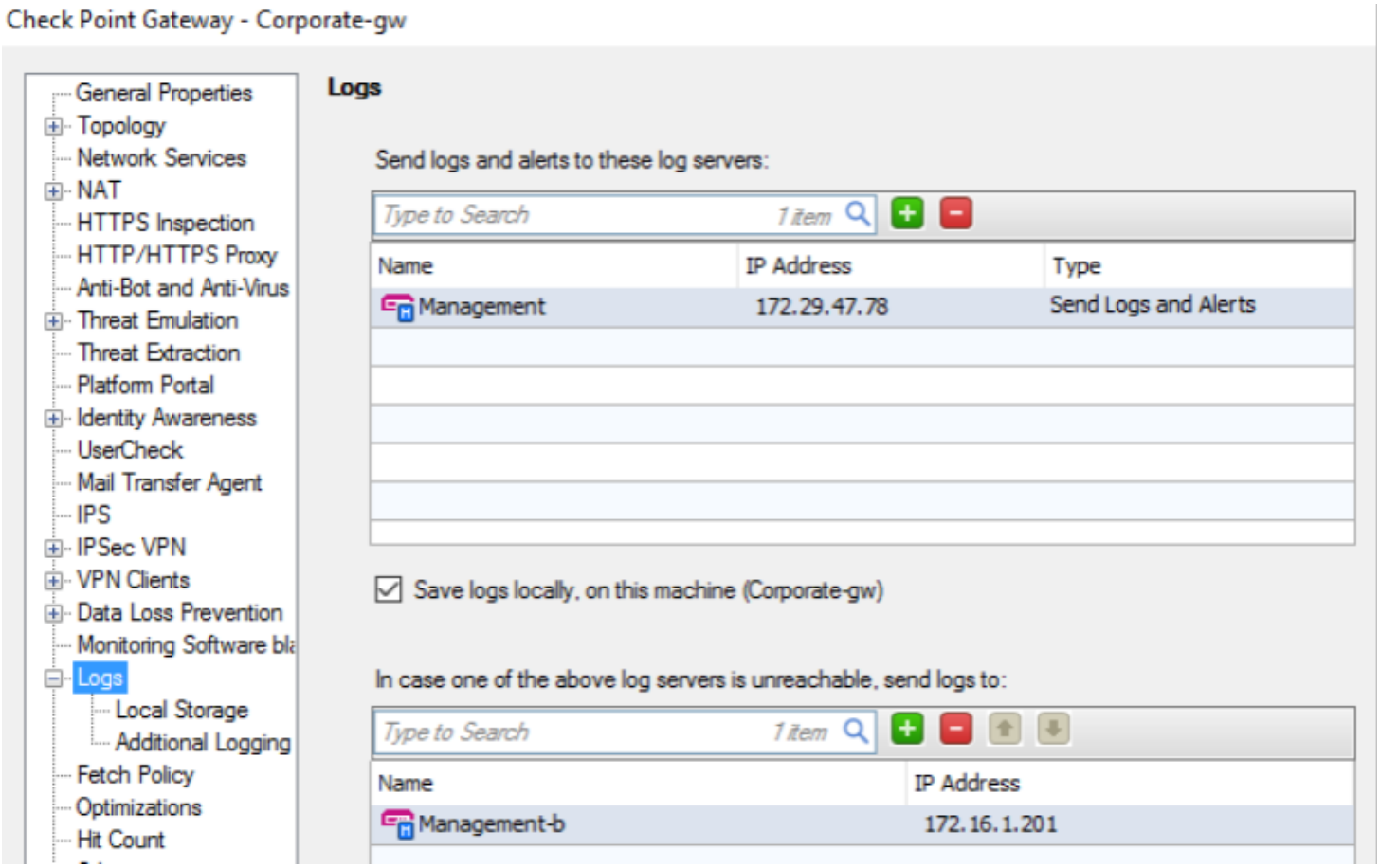


Рис. 2.11 Логирование

В качестве Лог-сервера может выступать сервер управления (Management Server) либо другое стороннее решение (возможно использование SIEM или Log Management систем).

13. На всех шлюзах настроен резервный Лог-сервер. Это позволит сохранить важные сообщения в случае отказа основного Лог-сервера.

14. На всех шлюзах также включена функция локального хранения логов. Это позволит сохранить информацию о событиях в случае недоступности Лог-сервер.

15. На всех шлюзах настроено создание нового Лог-файла при достижении определенного размера старого.

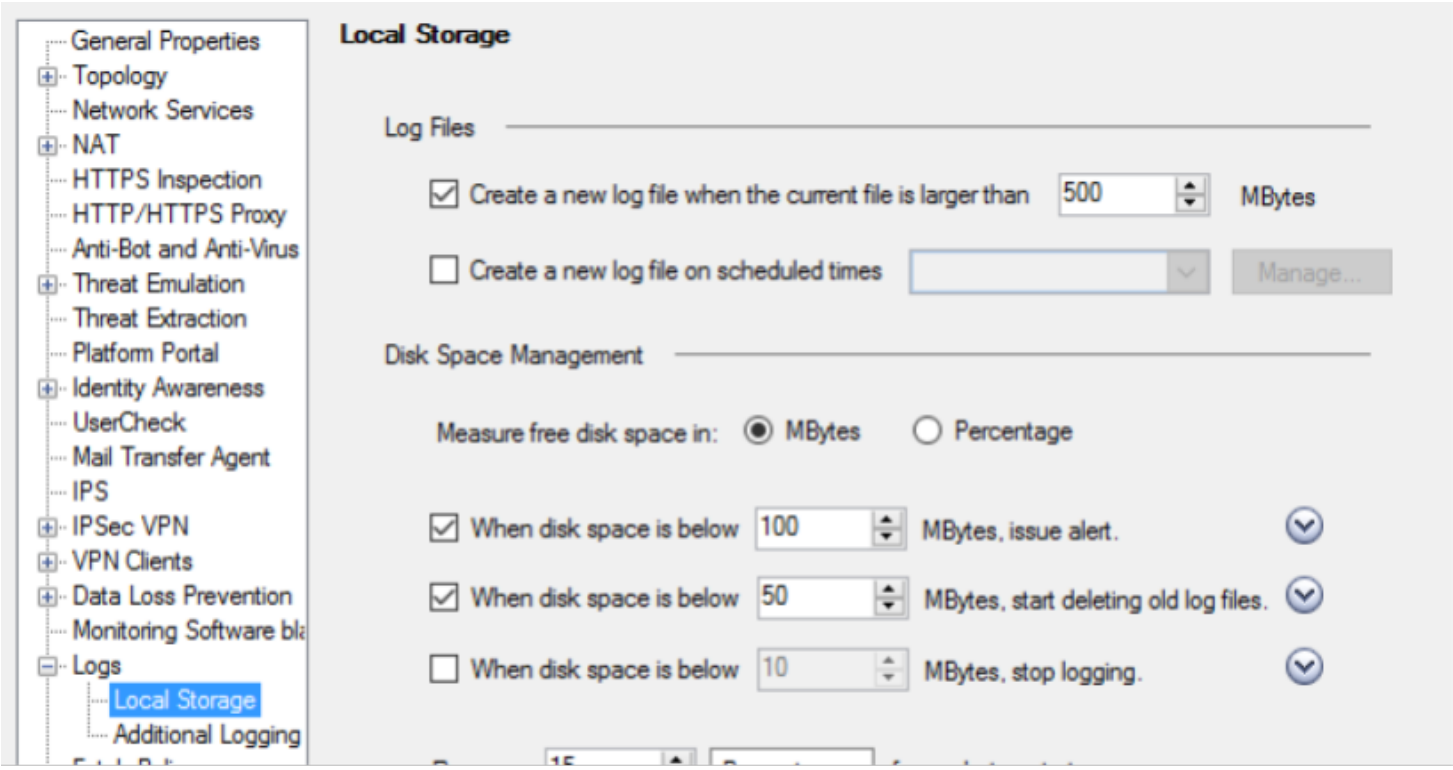


Рис. 2.12 Создание нового Лог-файла

Это значительно ускорит обработку логов (отображение, поиск). Вернуться к более старым логам можно будет переключив Лог-файл.

16. На всех шлюзах настроены уведомления сигнализирующие о заканчивающемся дисковом пространстве. Уровень срабатывания выбирается в зависимости от общего объема жесткого диска. Как правило порог выставляется в районе 50-100 МБайт.

17. На всех шлюзах настроено удаление старых Лог-файлов при заканчивающемся дисковом пространстве. Уровень срабатывания выбирается в зависимости от общего объема жесткого диска. Как правило порог выставляется в районе 50 МБайт.

18. На всех шлюзах настроены скрипты, которые выполняются перед удалением старых Лог-файлов.

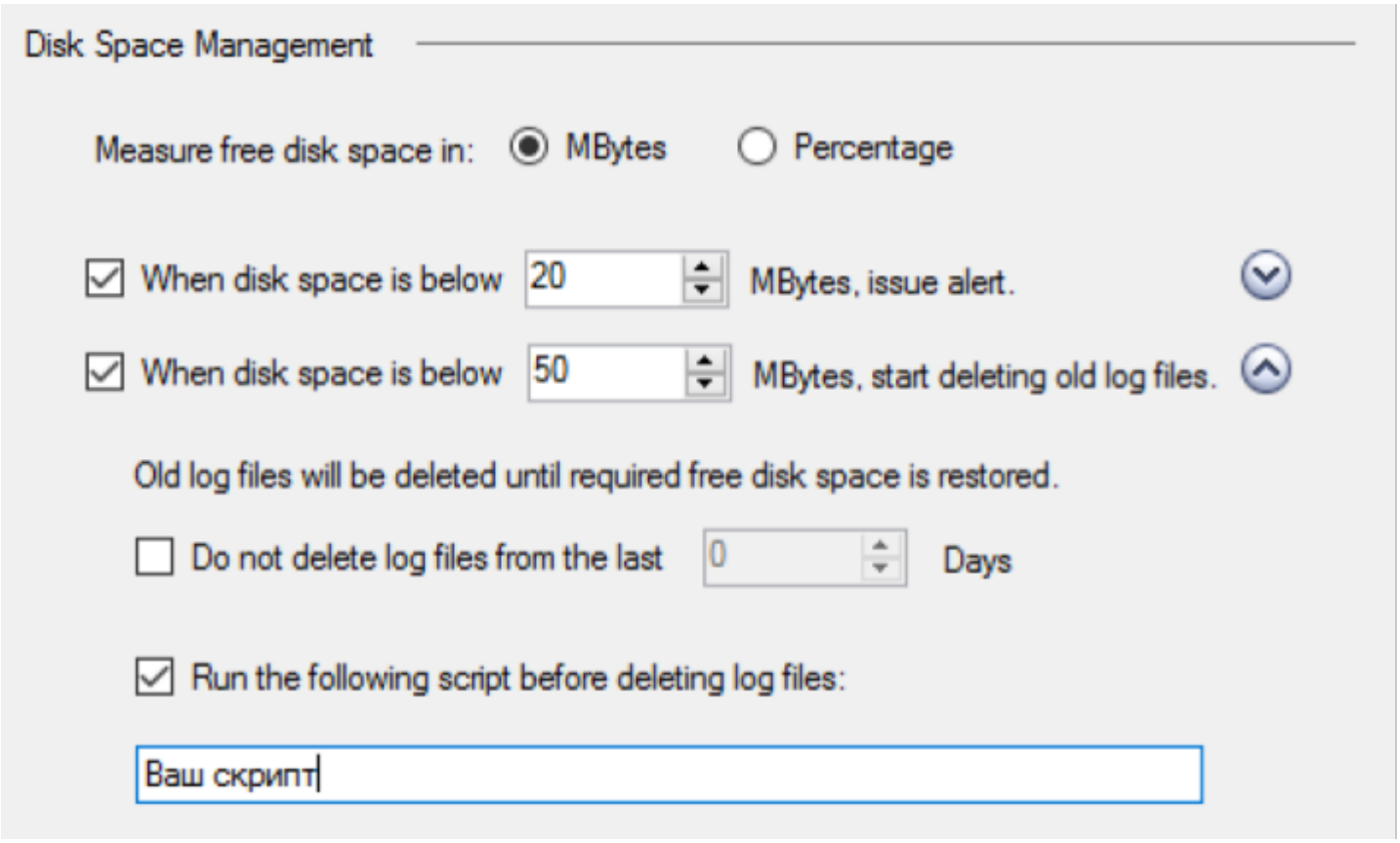


Рис. 2.13 Настроены скрипты, которые выполняются перед удалением старых Лог-файлов

С помощью данной функции можно убедиться, что созданы бэкапы логов.

19. В глобальных настройках включено логирование для “VPN packet handling errors”, “VPN successful key exchange”, “VPN configuration & key exchange errors”, “Administrative notifications”, “Packet is incorrectly tagged” и “Packet tagging brute force attack”:

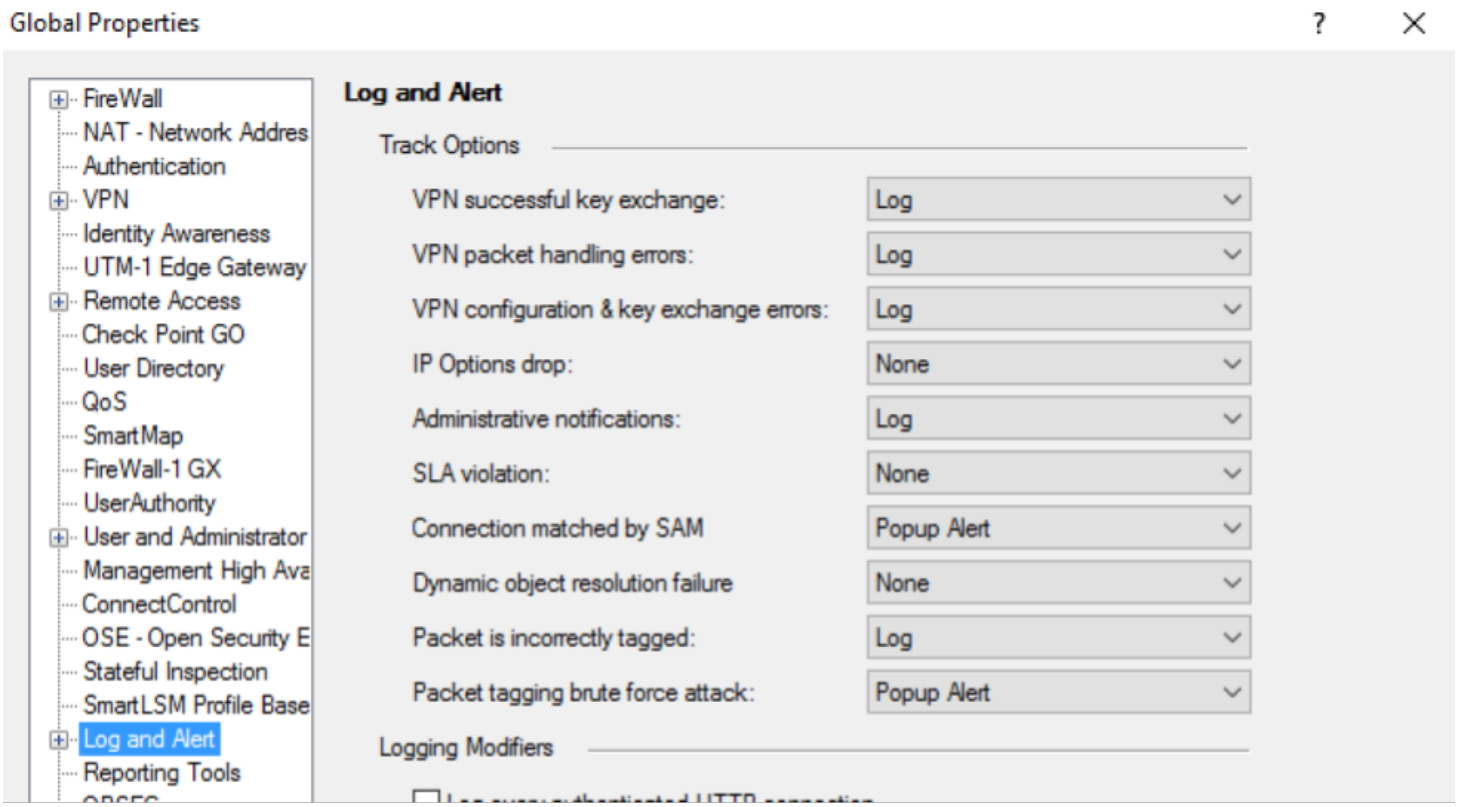


Рис. 2.14 Глобальные настройки

20. На всех шлюзах включен Anti-Spoofing в режиме prevent (для всех интерфейсов):

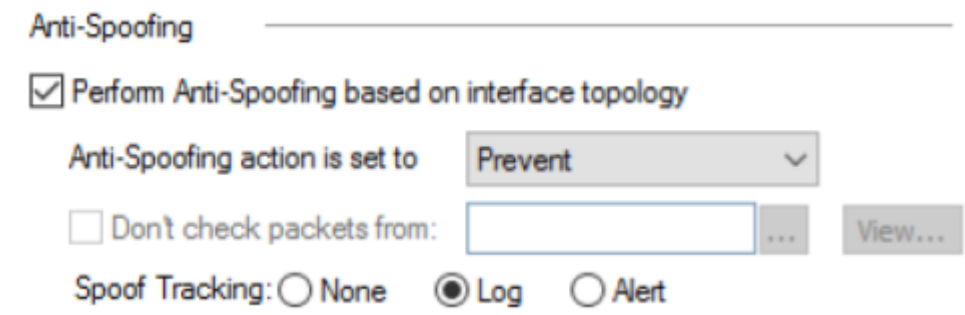


Рис. 2.15 Включен Anti-Spoofing в режиме prevent

21. В глобальных настройках (global properties) проверьте значения временных интервалов по умолчанию для stateful inspection:

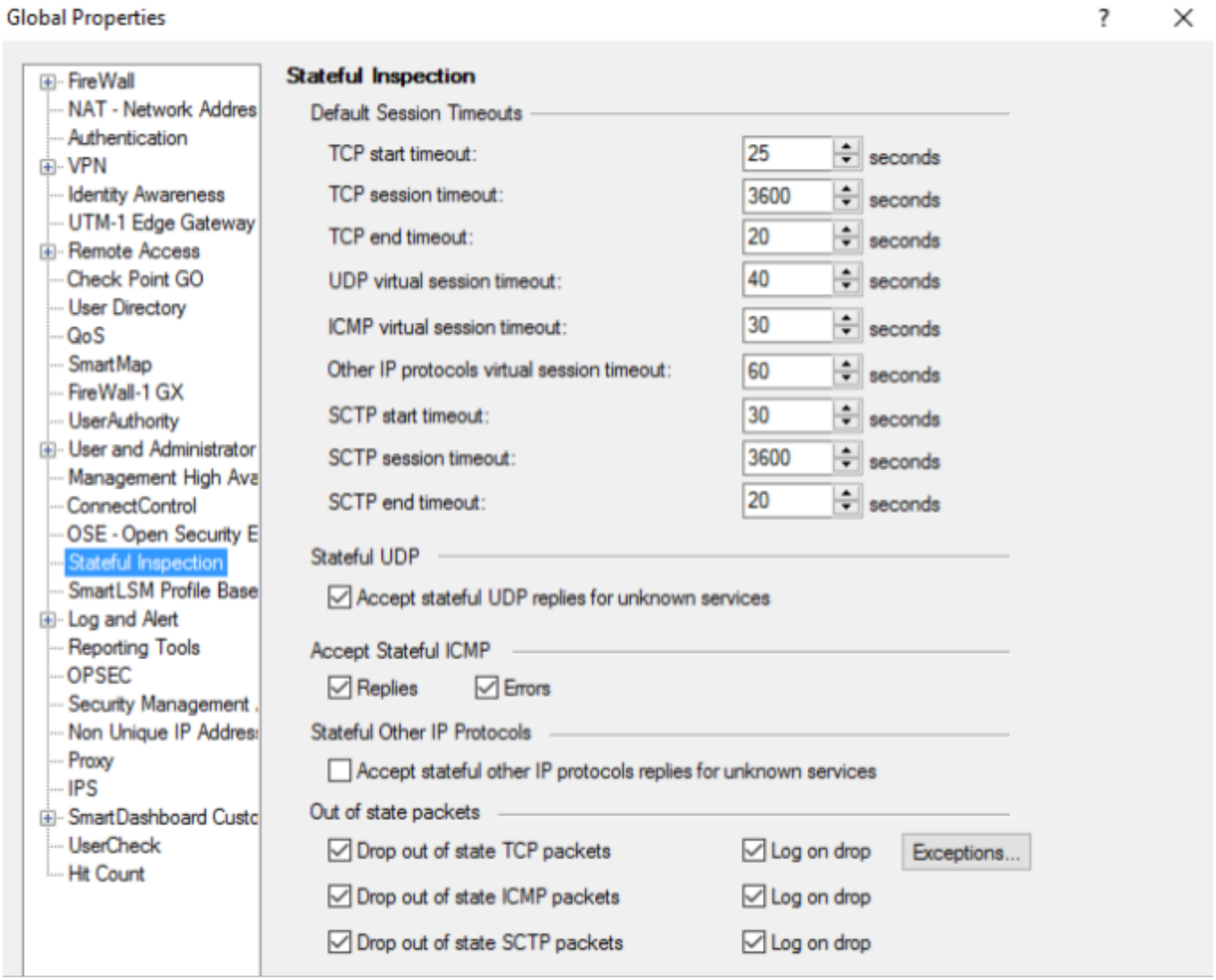


Рис. 2.16 Проверьте значения временных интервалов по умолчанию для stateful inspection

В случае необходимости измените в соответствии с требованиями вашей сети.

22. Для полей “Drop out of state TCP packets”, “Drop out of state ICMP packets” и “Drop out of state SCTP packets” включено Log on drop (смотри картинку выше).

23. В свойствах каждого шлюза включен счетчик Hit Count:

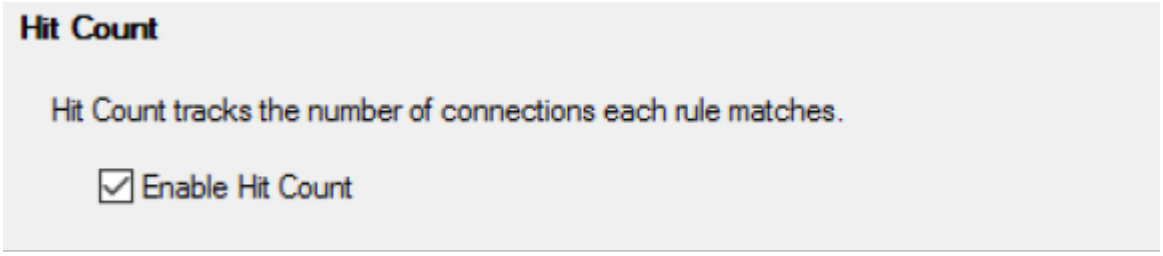


Рис. 2.17 Счетчик Hit Count

Это позволит видеть кол-во совпадений по каждому правилу (списку доступа) и удалять неиспользуемые.

24. В настройках оптимизации шлюза укажем максимальное количество конкурентных сессий.

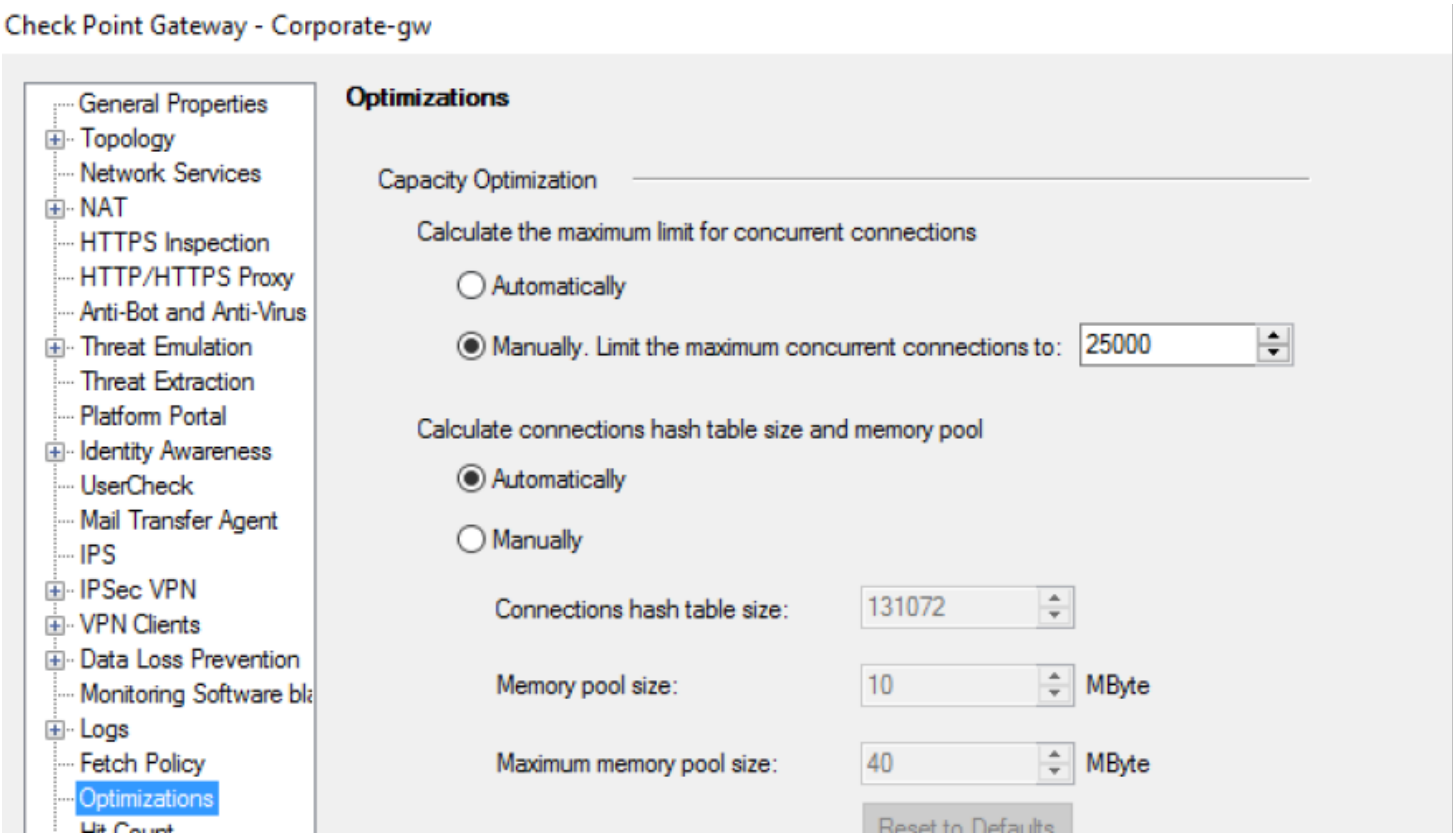


Рис. 2.18 Настройки автоматизации

Этот параметр зависит от модели шлюза и позволяет предотвратить перегрузку.

25. В глобальных настройках (global properties) пароли учетных записей пользователей (User Accounts) и администраторов (Administartor Accounts) истекают не позднее чем через 180 дней.

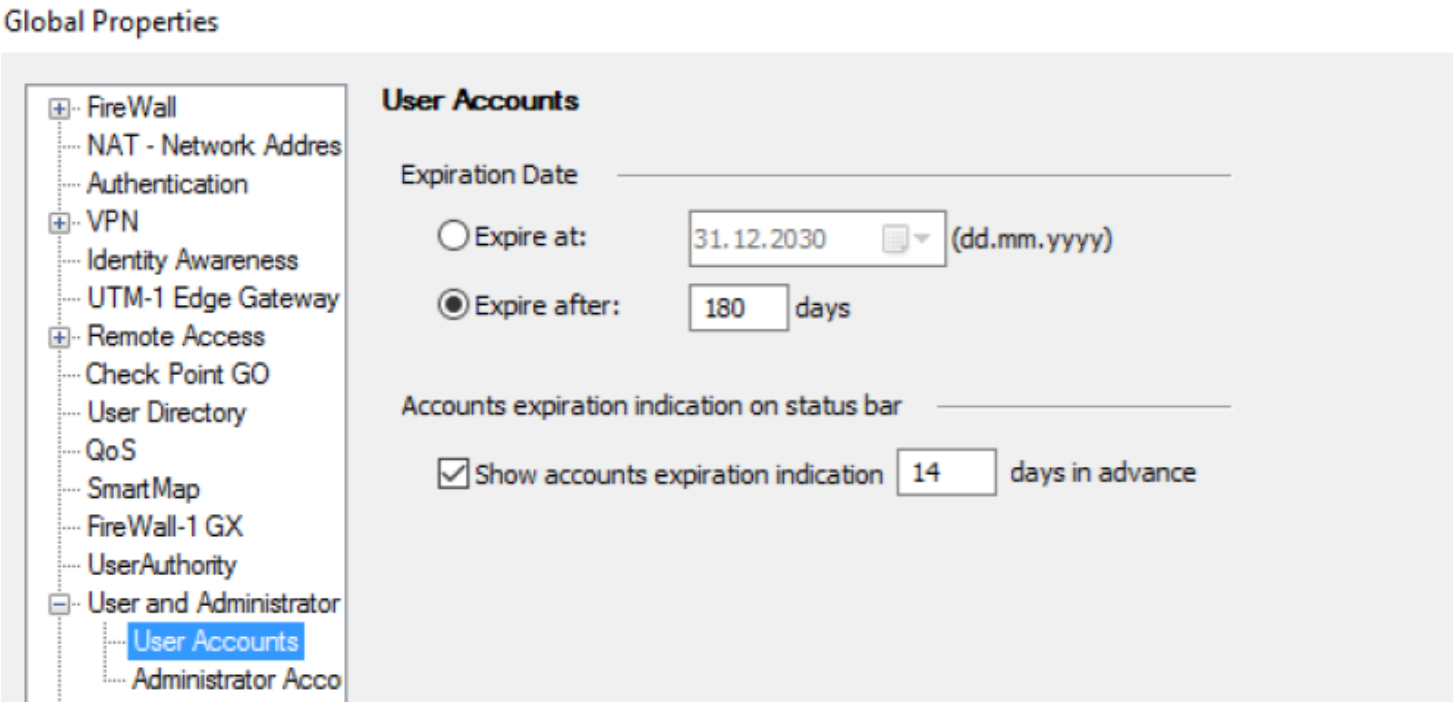
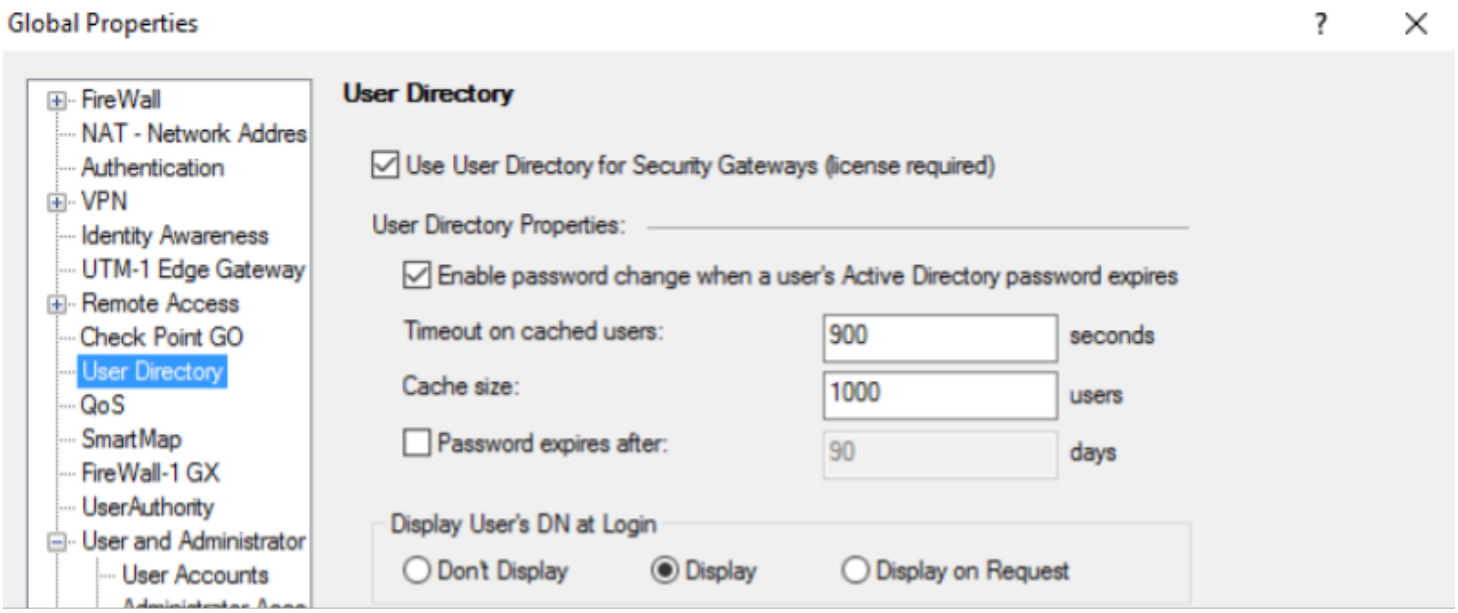


Рис. 2.19 Глобальные настройки

Также должно быть настроено оповещение об истекающем пароле.

26. При интеграции с Active Directory настроена смена пароля:



2.20 Смена пароля

27. В глобальных настройках (global properties) активирована блокировка Администраторов. Учетная запись блокируется на 30 минут в случае 3-х неудачных попыток входа.

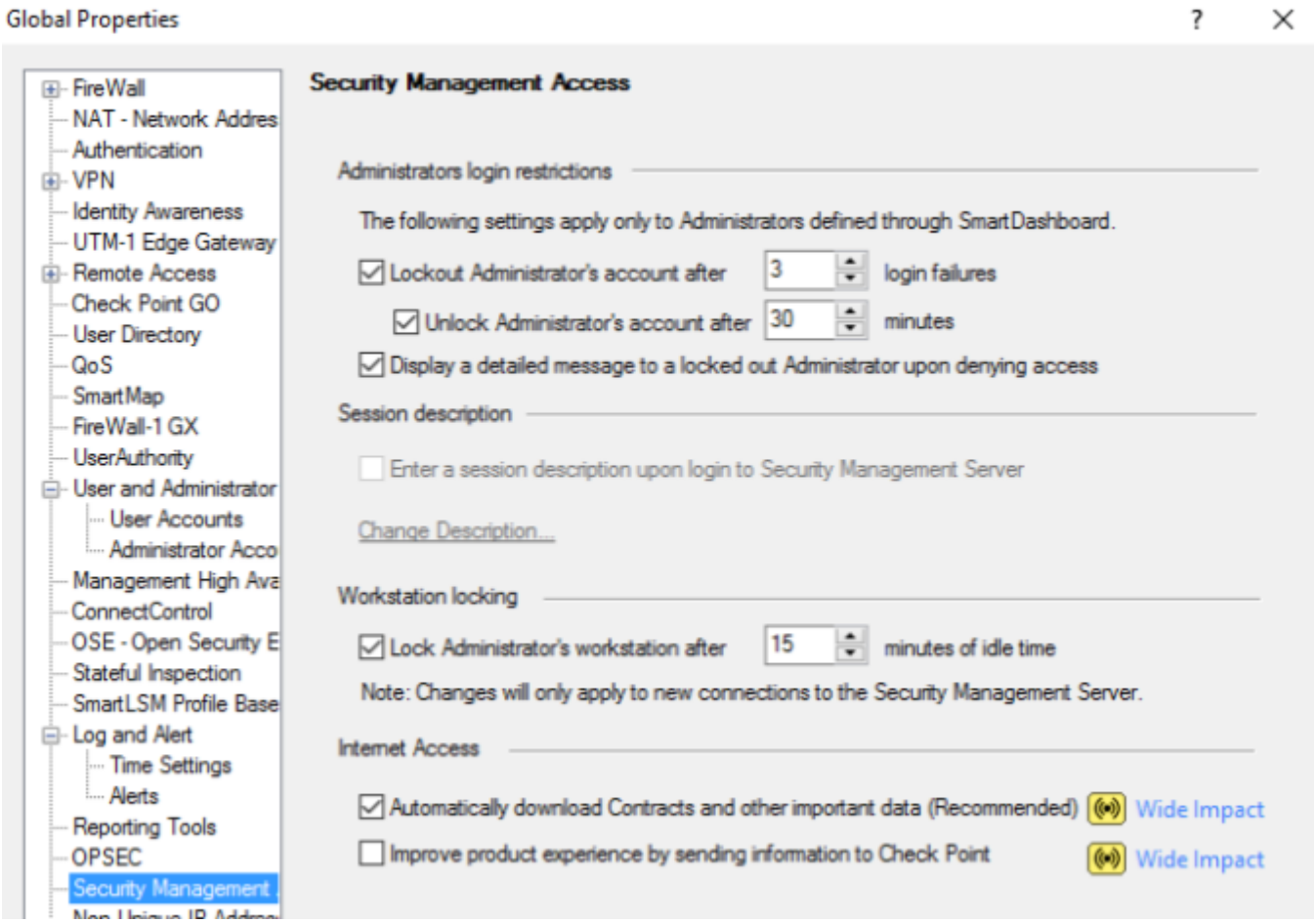


Рис. 2.21 Активирована блокировка Администраторов

Также настроено уведомление о блокировке и сброс сессии управления, неактивной в течении 15 минут.

28. В свойствах шлюзов выставлена опция “Rematch connections”.

Рис. 2.22 Свойство шлюзов

Это позволит блокировать запрещенные соединения сразу после установки новой политики и не ждать окончания сессии.

29. Настроена синхронизация времени (NTP)

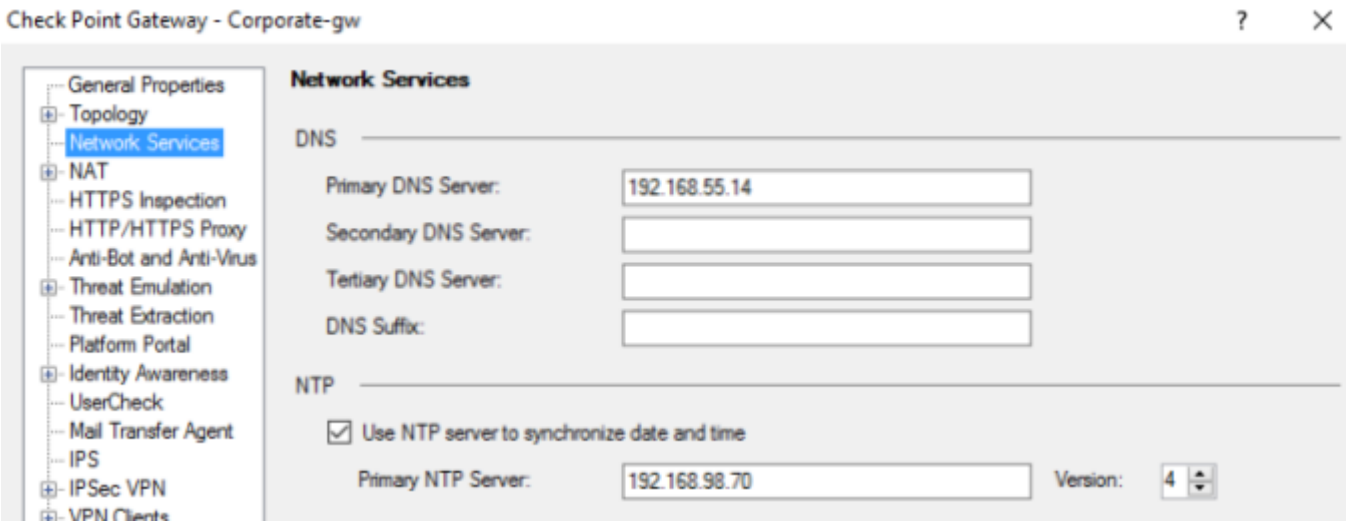


Рис. 2.23 Настройка синхронизация времени

Это позволит видеть актуальную дату и время для всех событий (логов).

Заключение

После всего изложенного материала можно заключить следующее.

На сегодняшний день лучшей защитой от компьютерных преступников является брандмауэр, правильно установленный и подобранный для каждой сети. И хотя он не гарантирует стопроцентную защиту от профессиональных взломщиков, но зато усложняет им доступ к сетевой информации, что касается любителей, то для них доступ теперь считается закрытым.

В процессе выполнения курсовой работы были изучены следующие вопросы:

Определение межсетевого экрана или брандмауэра

История создания брандмауэров

Фильтрация трафика

Классификация межсетевых экранов или брандмауэров

Формы межсетевых экранов

Реализация брандмауэров

Ограничения межсетевого экрана

Классы защищенности брандмауэров

Стандартизация брандмауэров

Настройка брандмауэров

Список литературы

1. О.Р. Лапонина. Межсетевое экранирование. «ИНТУИТ», М., 2009;
2. Девид Чемпен, Энди Фокс. Брандмауэры Cisco Secure PIX. «Вильямс», М., 2009;
3. Т.А. Биячуев. Безопасность корпоративных сетей. Спб., 2008;
4. А.Ю. Щеглов. Защита компьютерной сети от несанкционированного доступа. «НиТ», Спб., 2009;

5. Оглтри Firewalls. Практическое применение межсетевых экранов / Оглтри, Терри. - М.: ДМК Пресс, **2014**. - 400 с.
6. Рассел, Джесси Межсетевой экран / Джесси Рассел. - М.: Книга по Требованию, 2012. - 116 с.
7. Хендерсон, Лайза Межсетевое взаимодействие / Лайза Хендерсон , Том Дженкинс. - М.: Век +, Горячая Линия - Телеком, Энтроп, **2014**. - 316 с.
8. http://securitylab.ru
9. http://cisco.com
10. http://zonealarm.com
11. http://hub.ru